مجرمون إلكترونيون يطورون برمجية فدية خبيثة بسعر 175 دولارا

السبت 22 أبريل 2017 11:04 م

طور مجرمون إلكترونيون نسخةً جديدةً من برمجيات انتزاع الفدية الخبيثة، وأطلقوا عليها اسم "كارمن" Karmen، وهي متاحة في السوق السوداء مقابل 175 دولارًا أمريكيًا فقط.

وقالت شركة "ريكوردد فيوتشر" Recorded Future أمس الثلاثاء في منشور على مدونتها إن مستخدمًا يتحدث الروسية يُعرف باسم "ديف بيتوكس" DevBitox يُسوّق للبرمجية الخبيثة في منتديات الإنترنت السرية.

وأوضحت الشركة أن "كارمن" تنتمي إلى ما يسميه الخبراء الأمنيون "برمجيات انتزاع الفدية كخدمة" ransome-as-a-service، وهو اتجاه يوصف بأنه مثير للقلق على نحو خاص، ذلك أنه يمكن للقراصنة الهواة قليلي الخبرة التقنية شراؤها للوصول إليها، وفي المقابل، سوف تحصل هذه البرمجيات على مجموعة كاملة من الأدوات القائمة على الويب لتطوير هجمات انتزاع الفدية الخاصة بهم.

وفي حالة كارمن، فإن ذلك يوفر واجهة لوحة تحكم سهلة الاستخدام. يمكن للمشترين تعديل برمجية انتزاع الفدية الخبيثة، وعرض الأجهزة التي أُصيب لها، ومقدار المال الذي كسبوه.

يُذكر أنه لنشر برمجيات انتزاع الفدية الخبيثة، يعتمد المخترقون في كثير من الأحيان على رسائل البريد الإلكتروني غير المرغوب فيها "سبام" مع مرفق أو رابط إلى موقع ويب يحتوي على الترميز الخبيث. وبمجرد أن يُصاب جهاز الحاسب، فإن البرمجية الخبيثة تقوم بتشفير الملفات المستضافة على الجهاز. ولتحرير الملفات، يُضطر الضحايا لدفع فدية مالية، عادةً ما تُطلب بصغية عملة بيتكوين الرقمية.

وقد نشر "ديف بيتوكس"، وهو أحد مطوري "كارمن"، رسائل في مختلف المنتديات معلنًا عن توفر إصدارات باللغتين الروسية والإنجليزية من برمجية انتزاع الفدية الخبيثة كخدمة.

وبحسب شركة "ريكوردد فيتوتشر"، فقد تمكن القرصان الإلكتروني حتى الآن من بيع 20 نسخة من كارمن، وقد أشارت الشركة إلى أن العدوى الأولى بهذه البرمجية قد وقعت مطلع شهر كانون الأول/ديسمبر في ألمانيا والولايات المتحدة.

يُذكر أن موقع "نو مور رانسوم" أو "لا مزيد من الفدية" يختص بتوفير أدوات مجانية يمكن بواسطتها فك تشفير بعض أنواع برمجيات انتزاع الفدية الخبيثة. وكذا يوصي خبراء الأمن بأن تُجري الشركات عمليات جعل النسخ الاحتياطي الروتينية لأنظمتها المهمة.